



## DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549  
FORT MEADE, MARYLAND 20755-0549

IN REPLY  
REFER TO: Joint Interoperability Test Command (JTE)

**24 Apr 12**

**SUBJECT:** Extension of the Special Interoperability Test Certification of the Enterasys S Series S3 Switch from release 7.41.01.0013 to release 7.41.02.0014

References: (a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2005  
(b) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008  
(c) through (f), see Enclosure

1. References (a) and (b) establish the Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification.

2. The Enterasys S3-CHASSIS with release 7.41 is hereinafter referred to as the System Under Test (SUT). The SUT meets all of its critical interoperability requirements and is certified for joint use within the Defense Information System Network (DISN) as an Assured Services Local Area Network (ASLAN) distribution and Layer 2/Layer 3 access switch. The SUT is certified as interoperable for joint use with other ASLAN components listed on the Unified Capabilities (UC) Approved Products List (APL) with the following interfaces: 10/100/1000BaseT and 100/1000BaseX for access, 10/100/1000BaseT and 100/1000/10GBaseX for uplink. The SUT meets the critical interoperability requirements set forth in Reference (c), using test procedures derived from Reference (d). The Enterasys S3-CHASSIS-POE4 employs the same software and similar hardware as the SUT. JITC analysis determined this system to be functionally identical to the SUT for interoperability certification purposes, and it is also certified for joint use.

The SUT is certified to support DISN Assured Services over Internet Protocol. If a component meets the minimum requirements for deployment in an ASLAN, it also meets the lesser requirements for deployment in a non-ASLAN. Non-ASLANs are "commercial grade" and provide support to Command and Control (C2) (ROUTINE only calls) (C2(R)), or non-C2 voice subscribers. The SUT is certified for joint use deployment in a non-ASLAN for C2(R) and non-C2 traffic. When deployed in a non-ASLAN, the SUT may also be used to receive all levels of precedence but is limited to supporting calls that are originated at ROUTINE precedence only. Non-ASLANs do not meet the availability or redundancy requirements for C2 or Special C2 users and therefore are not authorized to support precedence calls originated above ROUTINE.

Testing of the SUT did not include video services or data applications; however, simulated video traffic, preferred data, and best effort data were generated during testing to determine the SUT's ability to prioritize and properly queue voice media and signaling traffic. No other configurations, features, or functions, except those cited within this document, are certified by JITC. This certification expires upon changes that affect interoperability but no later than three

JITC Memo, JTE, Extension of the Special Interoperability Test Certification of the Enterasys S Series S3 Switch from release 7.41.01.0013 to release 7.41.02.0014

years from the date of the signed Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL) approval Memorandum (12 December 2011).

3. The extension of this certification is based upon Desktop Review (DTR) 1. The original certification is based on interoperability testing conducted by the United States Army Information Systems Engineering Command, Technology Integration Center (USAISEC TIC), review of the vendor's Letters of Compliance (LoCs), and the DISA CA Recommendation. Interoperability testing was conducted by the USAISEC TIC, Fort Huachuca, Arizona, from 18 July through 26 August 2011 and documented in Reference (e). Review of the vendor's LoC was completed on 17 August 2011. The DISA CA provided a positive recommendation on 17 October 2011, based on the security testing completed by USAISEC TIC-led IA test teams. Those test results are published in a separate report, Reference (f). This DTR was requested to include release 7.41.02.0014. This release includes minor software changes related to commercial functionality and doesn't affect Assured Services. Therefore, JITC approves this DTR. The IA posture has not changed. The original IA approval applies to this DTR.

4. Table 1 provides the SUT's interface status. The SUT's capability and functional requirements are listed in Table 2.

**Table 1. SUT Interface Status**

Interface	Applicability			CRs/FRs (See note 1.)	Status		
	Co	D	A		Co	D	A
Network Management Interfaces for Core Layer Switches							
EIA/TIA-232 (Serial)	R	R	R	EIA/TIA-232	Met	Met	Met
IEEE 802.3i (10BaseT UTP)	C	C	C	1, 6-15, 18-28, 31, 32-36, 48-53, 58-60, 65, 67-71	Met	Met	Met
IEEE 802.3u (100BaseT UTP)	C	C	C	1, 6-15, 18-28, 31, 32-36, 48-53, 58-60, 65, 67-71	Met	Met	Met
IEEE 802.3ab (1000BaseT UTP)	C	C	C	1, 6-15, 18-28, 31, 32-36, 48-53, 58-60, 65, 67-71	Met	Met	Met
Uplink Interfaces for Core Layer Switches							
IEEE 802.3u (100BaseT UTP)	R	R	C <sup>2</sup>	1-15, 16, 18-24, 28-31, 40, 44-53, 55-60, 65-75	Met	Met	Met
IEEE 802.3u (100BaseFX)	C	C	C <sup>2</sup>	1-6, 11, 16, 18-24, 28-31, 40-41, 44-53, 55-60, 65-75	Met	Met	Met
IEEE 802.3ab (1000BaseT UTP)	C	C	C <sup>2</sup>	1-16, 18-24, 28-31, 40, 44-53, 55-60, 65-75	Met	Met	Met
IEEE 802.3z (1000BaseX Fiber)	R	R	C <sup>2</sup>	1-5, 8-16, 18-24, 28-31, 40, 44-53, 55-60, 65-75	Met	Met	Met
IEEE 802.3ae (10GBaseX)	C	C	C <sup>2</sup>	1-5, 8-16, 18, 19, 40-41, 44-53, 55-60, 65-75	Met	Met	Met
Access Interfaces for Core Layer Switches							
IEEE 802.3i (10BaseT UTP)	C	C	C <sup>2</sup>	1-15, 18-24, 28-41, 44-54, 58-71	Met	Met	Met
IEEE 802.3u (100BaseT UTP)	R	R	C <sup>2</sup>	1-15, 18-24, 28-41, 44-54, 58-71	Met	Met	Met
IEEE 802.3u (100BaseFX)	C	C	C <sup>2</sup>	1-6, 11, 18-24, 28-31, 44-54, 58-71	Met	Met	Met
IEEE 802.3ab (1000BaseT UTP)	C	C	C <sup>2</sup>	1-15, 18-24, 28-41, 44-54, 58-71	Met	Met	Met
IEEE 802.3z (1000BaseX Fiber)	R	R	C <sup>2</sup>	1-6, 11, 18-24, 28-31, 44-54, 58-71	Met	Met	Met
Generic Requirements for all Interfaces							
Generic Requirements not associated with specific interfaces	R	R	R	30-32, 35, 36, 40, 69-71	Met	Met	Met
DoD IPv6 Profile Requirements	R	R	R	UCR Section 5.3.5.5	Met	Met	Met
Security	R	R	R	UCR Sections 5.3.1.3.8, 5.3.1.5, 5.3.1.6, and 5.4	Met <sup>3</sup>	Met <sup>3</sup>	Met <sup>3</sup>

JITC Memo, JTE, Extension of the Special Interoperability Test Certification of the Enterasys S Series S3 Switch from release 7.41.01.0013 to release 7.41.02.0014

**Table 1. SUT Interface Status (continued)**

<b>NOTES:</b>			
1. The SUT's specific capability and functional requirement ID numbers depicted in the CRs/FRs column can be cross-referenced in Table 2. These requirements are for the following switch models, which are certified for Distribution and Layer 2/Layer 3 Access in the ASLAN: <b>S3-CHASSIS</b> , S3-CHASSIS-POE4. The devices listed that are not bolded or underlined are in the same family series as the SUT but were not tested. However, they utilize the same OS software and similar hardware as the SUT, and JITC analysis determined them to be functionally identical for interoperability certification purposes.			
2. Access layer switches are required to support only one of the following IEEE interfaces: 802.3i, 802.3j, 802.3u, 802.3ab, or 802.3z.			
3. Security testing is accomplished via USAISEC TIC-led IA test teams, and the results are published in a separate report, Reference (f).			
<b>LEGEND:</b>			
802.3ab	1000BaseT Gbps Ethernet over twisted pair at 1 Gbps (125 Mbps)	D	Distribution
802.3ae	10 Gbps Ethernet	DoD	Department of Defense
802.3i	10BaseT Mbps over twisted pair	EIA	Electronic Industries Alliance
802.3u	Standard for carrier sense multiple access with collision detection at 100 Mbps	EIA-232	Standard for defining the mechanical and electrical characteristics for connecting Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) data communications devices
802.3z	Gigabit Ethernet Standard		
10BaseT	10 Mbps (Baseband Operation, Twisted Pair) Ethernet	FR	Functional Requirement
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	IA	Information Assurance
100BaseFX	100 Mbps Ethernet over fiber	ID	Identification
1000BaseFX	1000 Mbps Ethernet over fiber	IEEE	Institute of Electrical and Electronics Engineers
1000BaseT	1000 Mbps (Baseband Operation, Twisted Pair) Ethernet	IPv6	Internet Protocol version 6
10GBaseX	10000 Mbps Ethernet over Category 5 Twisted Pair Copper	JITC	Joint Interoperability Test Command
A	Access	OS	Operating System
ASLAN	Assured Services Local Area Network	POE	Power over Ethernet
C	Conditional	R	Required
Co	Core	SUT	System Under Test
CR	Capability Requirement	TIA	Telecommunications Industry Association
		TIC	Technology Integration Center
		UCR	Unified Capabilities Requirements
		USAISEC	U.S. Army Information Systems Engineering Command
		UTP	Unshielded Twisted Pair

**Table 2. SUT Capability and Functional Requirements**

ID	Requirement (See note.)		UCR Reference
1	ASLAN components can have no single point of failure for >96 users for C2 and Special C2 users. Non-ASLAN components can have a single point of failure for C2(R) and non-C2 users. (R)		5.3.1.2.1, 5.3.1.7.7
2	Non-blocking of any voice or video traffic at 50% for core and distribution layer switches and 12.5% blocking for access layer switches. (R)		5.3.1.3
3	Maximum of 1 millisecond (ms) of jitter for voice and 10 ms for video for all ASLAN components. (R) Does not apply to preferred data and best effort data.		5.3.1.3
4	Maximum of 0.015% packet loss for voice and 0.05 % for video and preferred data for all ASLAN components. (R)		5.3.1.3
5	Maximum of 2 ms latency for voice, 10 ms for video, and 15 ms for preferred data for all ASLAN components. (R) Does not apply to best effort data.		5.3.1.3
6	100 Mbps IAW IEEE 802.3u and 1 Gbps IAW IEEE 802.3z for core and distribution layer components and only one of the following IEEE interfaces for access layer components: 802.3i, 802.3j, 802.3u, 802.3ab, or 802.3z. (R)		5.3.1.3.1
7	Force mode and auto-negotiation IAW IEEE 802.3, filtering IAW RFC 1812, and flow control IAW IEEE 802.3x. (R)		5.3.1.3.2
8	Port Parameter Requirements	Auto-negotiation IAW IEEE 802.3. (R)	5.3.1.3.2
9		Force mode IAW IEEE 802.3. (R)	
10		Flow control IAW IEEE 802.3x. (R)	
11		Filtering IAW RFC 1812. (R)	
12		Link Aggregation IAW IEEE 802.3ad (output/egress ports only). (R)	
13		Spanning Tree Protocol IAW IEEE 802.1D. (R)	
14		Multiple Spanning Tree IAW IEEE 802.1s. (R)	

**Table 2. SUT Capability and Functional Requirements (continued)**

ID	Requirement (See note.)		UCR Reference
15	Port Parameter Requirements (continued)	Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w. (R)	5.3.1.3.2
16	LACP link Failover and Link Aggregation IAW IEEE 802.3ad (uplink ports only) for core and distribution switches. (C)		5.3.1.3.2, 5.3.1.7.7.1
17	Class of Service Marking: Layer 3 DSCPs IAW RFC 2474 (R); Layer 2 3-bit user priority field of the IEEE 802.1Q 2-byte TCI field. (C)		5.3.1.3.3
18	VLAN capabilities IAW IEEE 802.1Q. (R)		5.3.1.3.4
19	Protocols IAW DISR profile (IPv4 and IPv6). IPv4 (R: LAN Switch, Layer 2 Switch): IPv6 (R: LAN Switch, C: Layer 2 Switch). Note: The Layer 2 switch is required to support only RFCs 2460, 5095, and 2464, and it must be able to queue packets based on DSCPs IAW RFC 2474.		5.3.1.3.5
20	QoS Features	Shall support minimum of 4 queues. (R)	5.3.1.3.6
21		Must be able to assign VLAN tagged packets to a queue. (R)	
22		Support DSCP PHBs per RFCs 2474, 2494, 2597, 2598, and 3246. (R: LAN Switch) Note: Layer 2 switch is required to support RFC 2474 only.	
23		Support a minimum of one of the following: Weighted Fair Queuing (WFQ) IAW RFC 3662, Priority Queuing (PQ) IAW RFC 1046, Custom Queuing (CQ) IAW RFC 3670, or Class-Based WFQ IAW RFC 3366. (R)	
24		Must be able to assign a bandwidth or a percentage of traffic to any queue. (R)	
25	Network Monitoring	SNMP IAW RFCs 1157, 2206, 3410, 3411, 3412, 3413, and 3414. (R)	5.3.1.3.7
26		SNMP traps IAW RFC 1215. (R)	
27		Remote monitoring IAW RFC 1281 and Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826. (R)	
28	Product Requirements Summary IAW UCR 2008, Table 5.3.1-5. (R)		5.3.1.3.9
29	E2E Performance (Voice)	No more than 6 ms Latency over any 5-minute period measured under 100% congestion. (R)	5.3.1.4.1
		No more than 3 ms Jitter over any 5-minute period measured under 100% congestion. (R)	
		Packet loss not to exceed .045% engineered (queuing) parameters over any 5-minute period under congestion. (R)	
30	E2E Performance (Video)	No more than 30 ms Latency over any 5-minute period measured under 100% congestion. (R)	5.3.1.4.2
		No more than 30 ms Jitter over any 5-minute period measured under congestion. (R)	
		Packet loss not to exceed 15% engineered (queuing) parameters over any 5-minute period under 100% congestion. (R)	
31	E2E Performance (Data)	No more than 45 ms Latency over any 5-minute period measured under congestion. (R)	5.3.1.4.3
		Packet loss not to exceed engineered (queuing) parameters over any 5-minute period under congestion. (R)	
32	LAN Network Management	Configuration Control for ASLAN and non-ASLAN. (R)	5.3.1.6.1
33		Operational Controls for ASLAN and non-ASLAN. (R)	5.3.1.6.2
34		Performance Monitoring for ASLAN and non-ASLAN. (R)	5.3.1.6.3
35		Alarms for ASLAN and non-ASLAN. (R)	5.3.1.6.4
36		Reporting for ASLAN and non-ASLAN. (R)	5.3.1.6.5
37	Redundancy	Redundant Power Supplies. (required on standalone redundant products)	5.3.1.7.7
38		Chassis Failover. (required on standalone redundant products)	
39		Switch Fabric Failover. (required on standalone redundant products)	
40		Non-LACP Link Failover. (R)	
41		Fiber Blade Failover. (R)	
42		Stack Failover. (C) (required if the stack supports more than 96 users)	
43		CPU (routing engine) blade Failover. (R)	
44	MPLS	MPLS may not add measurable Loss or Jitter to system. (C)	5.3.1.8.4.1
45		MPLS conforms to RFCs in Table 5.3.1-14. (C)	5.3.1.8.4.1
46		MPLS supports L2 and L3 VPNs. (C)	5.3.1.8.4.2.1/2
47	IPv6 Product Requirements: Dual Stack for IPv4 and IPv6 IAW RFC 4213 if routing functions are supported. (C)		5.3.5.4
48	IPv6 System Requirements	Support IPv6 IAW RFCs 2460 and 5095 if routing functions are supported. (C)	5.3.5.4
49		Support IPv6 packets over Ethernet IAW RFC 2464. (R)	5.3.5.4
50		Support MTU discovery IAW RFC 1981 if routing functions are supported. (R)	5.3.5.4.1
51		Support a minimum MTU of 1280 IAW RFCs 2460 and 5095. (C)	5.3.5.4.1
52		Shall support IPv6 addresses IAW RFC 4291. (R)	5.3.5.4.3
53		Shall support IPv6 scoped addresses IAW RFC 4007. (R)	5.3.5.4.3
54		If routing functions are supported: If DHCP is supported, it must be IAW RFC 3315; if DHCPv6 is supported, it shall be IAW RFC 3313. (C)	5.3.5.4.4
55	IPv6 Router Advertisements	If the system supports routing functions, the system shall inspect valid router advertisements sent by other routers and verify that the routers are advertising consistent information on a link, shall log any inconsistent router advertisements, and shall prefer routers that are reachable over routers whose reachability is suspect or unknown. (C)	5.3.5.4.5.2

**Table 2. SUT Capability and Functional Requirements (continued)**

ID	Requirement (See note.)		UCR Reference
56	IPv6 Router Advertisements (continued)	If the system supports routing functions, the system shall include the MTU value in the router advertisement message for all links IAW RFC 2461 and RFC 4861. (C)	5.3.5.4.5.2
57		IPv6 Neighbor Discovery: The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	
58	IPv6 Neighbor Discovery	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5
59		The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	
60		The system shall set the override flag bit in the neighbor advertisement message to “1” if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	
61	IPv6 SLAAC and Manual Address Assignment	If the system supports stateless IP address Auto-configuration, the system shall support IPv6 SLAAC for interfaces supporting UC functions IAW RFC 2462 and RFC 4862. (C)	5.3.5.4.6
62		If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the function to be enabled and disabled. (C)	
63		If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the “managed address configuration” flag and the “other stateful configuration” flag to always be set and not perform stateless auto-configuration. (C)	
64		If the product supports stateless IP address auto-configurations, including those provided for the commercial market, the DAD shall be disabled IAW RFC 2462 and RFC 4862. (R)	
65		The system shall support manual assignment of IPv6 addresses. (R)	
66		If the system provides routing functions, the system shall default to using the “managed address configuration” flag and the “other stateful” flag set to TRUE in the router advertisements when stateful auto-configuration is implemented. (C)	
67	IPv6 ICMP	The system shall support the ICMPv6 as described in RFC 4443. (R)	5.3.5.4.7
68		The system shall have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages. (R)	
69		The system shall support the capability to enable or disable the ability of the system to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion. (R) Required if LS supports routing functions.	
70		The system shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address. (R)	
71		The system shall validate ICMPv6 messages, using the information contained in the payload, prior to acting on them. (R)	
72	IPv6 Routing Functions	If the system supports routing functions, the system shall support the OSPF for IPv6 as described in RFC 5340. (C)	5.3.5.4.8
73		If the system supports routing functions, the system shall support securing OSPF with Internet Protocol Security (IPSec) as described for other IPSec instances in UCR 2008, Section 5.4. (C)	
74		If the system supports routing functions, the system shall support OSPF for IPv6 as described in RFC 2740, router-to-router integrity using an IP authentication header with HMAC-SHA1-96 with ESP and AH as described in RFC 2404, and shall support OSPFv3 IAW RFC 4552. (C)	
75		If the system supports routing functions, the system shall support the Multicast Listener Discovery (MLD) process as described in RFC 2710 and extended in RFC 3810. (C)	
76	Site Requirements	Engineering Requirements: Physical Media for ASLAN and non-ASLAN. (R) (Site requirement)	5.3.1.7.1
77		Battery back-up: two hours for non-ASLAN components and eight hours for ASLAN components. (R) (Site requirement)	5.3.1.7.5
78		Availability of 99.999% (Special C2), 99.997% (C2) for ASLAN (R), and 99.9% (non-C2 and C2(R)) for non-ASLAN. (R) (Site requirement)	5.3.1.7.6
79	IA Security Requirements	Port-Based Access Control IAW IEEE 802.1x and 802.3x. (R)	5.3.1.3.2
80		Secure methods for network configuration: SSH2 instead of Telnet and support RFCs 4251-4254. Must use HTTPS instead of http and support RFCs 2660 and 2818 for ASLAN and non-ASLAN. (R)	5.3.1.6
81		Security. (R)	5.3.1.3.8
82		Must meet IA requirements IAW UCR 2008 Section 5.4 for ASLAN and non-ASLAN. (R)	5.3.1.5
NOTE: All requirements are for core, distribution, and access layer components unless otherwise specified.			

**Table 2. SUT Capability and Functional Requirements (continued)**

<b>LEGEND:</b>					
AH	Authentication Header	HTTP	Hypertext Transfer Protocol	OSPFv3	Open Shortest Path First Version 3
ASLAN	Assured Services Local Area Network	HTTPS	Hypertext Transfer Protocol, Secure	PHB	Per Hop Behavior
C	Conditional	IA	Information Assurance	QoS	Quality of Service
C2	Command and Control	IAW	in accordance with	R	Required
C2(R)	Command and Control ROUTINE only	ICMP	Internet Control Message Protocol	RFC	Request for Comments
CPU	Central Processing Unit	ICMPv6	Internet Control Message Protocol for IPv6	SHA	Secure Hash Algorithm
DAD	Duplicate Address Detection	ID	Identification	SLAAC	Stateless Auto Address Configuration
DHCP	Dynamic Host Configuration Protocol	IEEE	Institute of Electrical and Electronics Engineers	SNMP	Simple Network Management Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6	IPv4	Internet Protocol version 4	SSH2	Secure Shell Version 2
DISR	Department of Defense Information Technology Standards Registry	IPv6	Internet Protocol version 6	SUT	System Under Test
DSCP	Differentiated Services Code Point	LACP	Link Aggregation Control Protocol	TCI	Tag Control Information
E2E	End-to-End	LAN	Local Area Network	UC	Unified Capabilities
ESP	Encapsulating Security Payload	LS	LAN Switch	UCR	Unified Capabilities Requirements
Gbps	Gigabits per second	Mbps	Megabits per second	VLAN	Virtual Local Area Network
HMAC	Hash-based Message Authentication Code	MPLS	Multiprotocol Label Switching	VPN	Virtual Private Network
		ms	millisecond		
		MTU	Maximum Transmission Unit		
		OSPF	Open Shortest Path First		

5. In accordance with the Program Manager's request, no detailed test report was developed. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Non-Secure Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet). Information related to DISN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly from U.S. Government civilian or uniformed military personnel at the Unified Capabilities Certification Office (UCCO); e-mail: [ucco@disa.mil](mailto:ucco@disa.mil).

6. The JITC point of contact is Mr. Edward Mellon, DSN 879-5159, commercial (520) 538-5159, FAX DSN 879-4347, or e-mail to [Edward.Mellon@disa.mil](mailto:Edward.Mellon@disa.mil). JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The Tracking Number for the SUT is 1035401.

FOR THE COMMANDER:

Enclosure a/s

  
for BRADLEY A. CLARK  
Chief  
Battlespace Communications Portfolio

JITC Memo, JTE, Extension of the Special Interoperability Test Certification of the Enterasys S Series S3 Switch from release 7.41.01.0013 to release 7.41.02.0014

DISTRIBUTION (electronic mail):

Joint Staff J-6

Joint Interoperability Test Command, Liaison, TE3/JT1

Office of Chief of Naval Operations, CNO N6F2

Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)

Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT),  
SAIS-IOQ

U.S. Marine Corps MARCORSYSCOM, SIAT, MJI Division I

DOT&E, Net-Centric Systems and Naval Warfare

U.S. Coast Guard, CG-64

Defense Intelligence Agency

National Security Agency, DT

Defense Information Systems Agency, TEMC

Office of Assistant Secretary of Defense (NII)/DOD CIO

U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities  
Division, J68

Defense Information Systems Agency, GS23

**This page intentionally left blank.**



## **ADDITIONAL REFERENCES**

- (c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 2," 31 December 2010
- (d) Joint Interoperability Test Command, "Defense Switched Network Generic Switch Test Plan (GSTP), Change 2," 2 October 2006
- (e) Joint Interoperability Test Command, Memo, JTE, "Special Interoperability Test Certification of the Enterasys S Series S3 Switch with release 7.41.," 6 December 2011
- (f) U.S. Army Information Systems Engineering Command (HQUSAISEC), Technology Integration Center (TIC), "Information Assurance (IA) Assessment of Enterasys S Series S3 Switch (Tracking Number 1035401)," 17 October 2011